In the Specification:

Please amend the specification as set forth below. Paragraph numbers are as per the published application, since the application as filed did not include paragraph numbers.

[0106] In this embodiment the user [[24]] 25 (now the sender) on the network 28 wishes to send an outbound message to a user [[22]] 23 (now the recipient) on the insecure network 10. The user [[24]] 25 wishes to ensure the contents of the message remains confidential, even while in transit over the network 28 which may be secure or insecure. If the network 28 is secure the sender may require further security than that which is provided on the network 28.

[0107] The user [[24]] 25 generates the message using the secure e-mail client [[18]] 19 on the network 28. The user [[24]] 25 specifies at the e-mail client [[18]] 19 the user's [[22]] 23 e-mail address and specifies that the message is to be encrypted.

[0108] Prior to transmission, the e-mail client 18 performs an authenticated request 60 for the public key container(s) of the user [[22]] 23 against the directory 20.

[0109] The directory 20 determines that the request has originated from a client within the network 28 and then generates an encryption key container in response. This key container embeds the secure e-mail gateway's 14 public encryption key and the user's [[22]] 23 e-mail address. This key container is transmitted 62 to the e-mail client [[18]] 19.

[0110] The e-mail client [[18]] 19 may or may not be aware that the key container it received does not contain the public key of the user [[22]] 23. The e-mail client [[18]] 19 verifies the integrity and authenticity of the key container and if satisfied it has been generated from a trustworthy source then uses the public key embedded within the received key container to encrypt the message.

[0111] The secure e-mail client [[18]] 19 then transmits 64 the encrypted message to the user [[22]] 23. The mail system on the network 28 routes the message to the secure e-mail gateway 14.

[0113] The secure e-mail gateway 14 then transmits the message to the user [[22]] 23. The message may be transmitted in this decrypted state. Alternatively, the secure e-mail gateway 14 can re-encrypt the message using the user's [[22]] 23 genuine public key.

[0114] The mail system on the insecure network 10 routes the message to the user's [[22]] 23 email client 16. The user [[22]] 23 can then retrieve and read the message.

[0116] In this embodiment the user [[24]] 25 (the sender) on the secure network 12 wishes to send a message to a user [[22]] 23 (the recipient) on the insecure network 10. The user [[24]] 25 wishes the user [[22]] 23 to be able to verify the message has originated from the user's [[22]] 23 message domain and to be assured that it has retained its integrity while in transit over the insecure network 10.

[0117] The user [[24]] 25 generates the message using the e-mail client [[18]] 19 on the secure network 12. The user [[24]] 25 specifies the user's [[22]] 23 e-mail address and transmits 80 the message to the user [[22]] 23. The user [[24]] 25 also indicates that the message should retain its authenticity and integrity while on the insecure network 10. The user [[24]] 25 may make this indication by including in the subject line of the e-mail a predetermined string of characters or selecting the option within the e-mail client, such as ticking a check box. The mail system on the secure network 12 routes the message to the secure e-mail gateway 14.

[0118] The secure e-mail gateway 14 signs the message with its private signing key. It performs an authenticated request 84 against the directory 20 for the public key container(s) of the user [[24]] 25.

[0119] The directory 20 determines that the request has originated from the user [[24]] 25 domain's secure e-mail gateway 14 and in consequence generates a signing public key container in response. This key container embeds the secure e-mail gateway's 14 public signing key and the sender's e-mail address, and a parameter that indicates the container is for use with digital signature operations. The directory 20 then transmits 86 the key container to the secure e-mail gateway 14.

[0120] The secure e-mail gateway 14 embeds the key container within the signed message that has been created with the private signing key. The secure e-mail gateway 14 transmits 88 the message and the signing public key container to the user [[22]] 23 across the insecure network 10.

[0121] The user [[22]] 23 retrieves the message using the secure e-mail client 16 on the insecure network 10. The secure e-mail client 16 verifies the authenticity and integrity of the message by performing a digital signature verification operation.

[0127] A ~~requester~~ requestor 108 initiates the provision of public key containers. The ~~requester~~ requestor 108 could be a secure e-mail gateway 12 or a secure e-mail client 16.